REMARKS

Applicant has carefully reviewed the Final Office Action mailed August 23, 2006 and offers the following remarks.

Applicant wishes to thank the Examiner for indicating that claims 1-6, 8, and 9 are allowed.

Before addressing the substance of the rejections, Applicant provides a brief overview of the present invention. The present invention is a tunneling scheme that goes beyond conventional tunneling between two endpoints. The present invention involves a tunnel for private communications that is stretched over two sub-endpoints each having an address in order to provide separation between the end user address space and the carrier address space when performing VPN communications. (Specification, p. 4, ll. 1-2). By dividing the endpoint of a given tunnel into two sub-endpoints, the tunneling scheme is able to reduce the likelihood of a security threat that can occur in the case of a mis-provisioning of a traditional VPN. (Specification, p. 11, ll. 3-6). This is opposed to traditional tunneling schemes that encapsulate a packet with the identity of the endpoints of the tunnel thereby providing the destination address of an endpoint of the tunnel that may not be desired to be seen by the outside world. (Specification, p. 3, ll. 6-9).

An example of the present invention is provided with respect to a private source endpoint on a first private data network that desires to communicate a message to a private destination endpoint on a second private data network to accomplish VPN communications. References are made to Figure 10 to assist in the understanding of the example. First, the private source endpoint communicates the desired message and the private destination address over its private network (LAN A - 108A) to an intermediary local carrier router (216M) acting as a first sub-endpoint. The local carrier router (216M) contains a backbone router (BR – 204M) that has a public address and a number of virtual routers (CVR - 206A) for connecting to LANs (108A). The local carrier router (216M) reads the private destination address and determines a private address of a private remote sub-endpoint (CVR – 206X) of a communication tunnel. The private remove sub-endpoint (CVR - 206X) is associated with the private destination address on a remote private network (LAN X - 108X).

Traditional tunneling would stop at this point and encapsulate the message with the source as the local carrier router (216M) public address and the destination as the private

designation address (CVR - 206X) thereby exposing the private destination address to the outside world. Instead, for the present invention, the local carrier router (216M) determines a public address of a public remote sub-endpoint (216N) of the tunnel that provides the second sub-endpoint in the tunnel. The local carrier router (216M) then encapsulates the message with a source address as a public local sub-endpoint (204M) of the tunnel and a destination address as the public remote sub-endpoint (216N) of the tunnel. The private destination address is provided in the inner encapsulated part of the message rather than being exposed in the outer source or destination addresses like in traditional tunneling.

Thus in summary, the present invention provides two sub-endpoints for providing the tunneling communication scheme where both the source and destination of the encapsulated message are not the private addresses of the private endpoints. Traditional tunneling does not provide two sub-endpoints. Thus, the destination address of the encapsulated message is a private address. Because VPN communications are two-way, traditional tunneling exposes the private destination addresses of both endpoints. The present invention does not.

Claim 7 was rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,636,516 B1 to Yamano (hereinafter "Yamano"). Applicant respectfully traverses. For a reference to be anticipatory, the reference must disclose each and every claim element. Further, the elements of the reference must be arranged as claimed. MPEP § 2131. The requirement that each and every element be disclosed in the manner claimed is a rigorous standard that the Patent Office has not met in this case.

In response to Applicant's previous arguments that Yamano does not disclose two sub-endpoints, the Patent Office asserts that claim 7 does not recite two, distinct sub-endpoints (Final Office Action mailed August 23, 2006, p. 3). Applicant traverses. Claim 7 recites a carrier router comprising:

a backbone router including:

a public network interface for connecting to a public data network; and

a sub-endpoint for a tunnel <u>having a network address in an address space of said public data network</u>; and

a customer virtual router including:

a private network interface for connecting to a private data network; and

a sub-endpoint for said tunnel <u>having a network address in an address space of said private data network</u>.

As seen in the emphasized portions of claim 7 above, two sub-endpoints are claimed for the communication tunnel. The first sub-endpoint is provided in a backbone router than has a network address in a public data network. The second sub-endpoint is provided in a virtual router that has a network address in a private data network. Since the first sub-endpoint is provided in a backbone router and has an address in a public data network and the second sub-endpoint is provided in a customer virtual router and has an address in a private data network, the two sub-endpoints are obviously distinct. In light of this fact, and as discussed below, the fact that Yamano does not disclose two sub-endpoints, Yamano cannot anticipate claim 7.

The Patent Office asserts that Yamano discloses the claimed invention at col 3., lines 42-48 and Figures 2 and 3 (Final Office Action mailed August 23, 2006, p. 2). Yamano does disclose using a tunneling unit (305, see also Fig. 3) that provides tunneling of communications from a private network interface (301) to a public network interface (309). However, Yamano merely discloses the traditional tunneling described above that does not employ two sub-endpoints as claimed in the present invention. This is further evidenced by Yamano's use of the address translation table (306, see also Fig. 7) that provides only one intermediary address (Internet IP address) for a destination address. Thus, Yamano does not teach the two claimed sub-endpoints, and therefore does not anticipate, teach, or suggest the claimed invention, including claim 7, and this rejection must be withdrawn.

Claims 10 and 11 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2002/0038419 A1 to Garrett et al. (hereinafter "Garrett"). Applicant respectfully traverses. The standards for anticipation are set forth above. Claims 10 and 11 require two sub-endpoints to provide the modified communication tunneling as previously described. The Patent Office cites to paragraphs 0017 and 0019, as well as Figures 4, 6, and 7, of Garett as teaching the elements of claims 10 and 11 (Final Office Action mailed August 23, 2006, p. 3). However, just like Yamano, Garrett only discloses traditional communication tunneling that does not employ two sub-endpoints. This is evidenced by Garrett's disclosure in paragraphs 0016, 0017, and 0019. In paragraph 0016, Garrett states that traditional IP encapsulation is used for communication tunneling. In particular, see paragraph 0016, lines 12-14, where Garrett states that the outer source IP address and destination IP address

for the encapsulated message identify the endpoints of the tunnel. Paragraph 0017 states that the packet is encapsulated using the "encapsulation techniques described above" (i.e., meaning in paragraph 0016). Paragraph 0019 noted by the Patent Office actually states that tunneling need not be used.

In its response to Applicant's previous arguments that Garrett does not disclose two sub-endpoints, the Patent Office argues that "Garrett discloses receiving a packet with a destination address at the router (first end-point) and de-encapsulates the packets and then forwards the packet to the original destination address (second end-point) field after decapsulating the packet." (Final Office Action mailed August 23, 2006, p. 4). Garrett discloses endpoints of a tunnel and does not disclose **sub**-endpoints. Garrett merely discloses traditional tunneling where the source IP address and the destination IP address identify the endpoints of the tunnel. Endpoints of a traditional tunnel are not equivalent to the claimed **sub**-endpoints. As described in the specification at page 3, lines 25-27, the present invention envisions a traditional tunnel endpoint being stretched over two sub-endpoints, each with an address. Garrett does not disclose that its endpoints have two sub-endpoints, one with a public destination address and one with a private destination address, as required in claims 10 and 11. Thus, Garrett does not teach or suggest the claimed sub-endpoints. Moreover, Garrett does not disclose removing the public source and destination addresses from the packet **at the first sub-endpoint having said public destination address**, as required by both claims 10 and 11. Thus, since Garrett does not disclose two sub-endpoints and does not disclose removing the public source and destination addresses from the packet at the first sub-endpoint, it is clear that Garrett does not anticipate, teach, or suggest the claim limitations of claims 10 and 11. Thus, this rejection must be withdrawn.

The present application is now in condition for allowance and such action is respectfully requested. The Examiner is encouraged to contact Applicant's representative regarding any remaining issues in an effort to expedite allowance and issuance of the present application.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By: John R. Witcher, III

John R. Witcher, III
Registration No. 39,877
P.O. Box 1287
Cary, NC 27512
Telephone: (919) 654-4520

Date: October 23, 2006
Attorney Docket: 7000-497